Research paper on virtual machine security

Law, Security

Virtual Machine Security

Virtual machines represent completely isolated guest operating system installations in normal host operating systems (Griffin, 2006). Today they are implemented with the help of either hardware virtualization or software emulation. Often these two ways are combined so as to achieve more effective results. Although it is convenient to use such machines in different circumstances, there are certain issues with them in the field of security and some other areas (Kusnetzky, 2009; Whitehouse, 2011). In this paper I will describe one of the major security problems with virtual machine security, which is data protection in transit and storage.

The same problem of data protection exists in the case of physical machines as well, and VMs partly share the same issues, but also have the ones specific only for them (Araujo, & Hau, 2008; Double-Take, 2006). Some of the typical solutions work for the virtual environment and can be successfully used in it. Among them there are encryption, hashing and special protocols, such as SSL. When setting up the VMs, it is important to bear in mind that there may be required to enable more software components and services, than it was expected. In this case it is important not to miss the issue of protection and pay enough attention to it.

Among the issues that are unique for the virtualization area there is security of information that is stored directly on the host. The main problem is that typical virtual disk formats store the data in plain text, thus providing an easy way for attackers to access the information. Apart from this, virtual machines are more vulnerable to malware infections, as it is harder to find the origin of the problem and solve it (Garfinkel & Rosenblum, 2005; “

Virtualization Support," 2008).

On the whole, in order to prevent these risks, it is important to come up with strong access controls and properly encrypt the most sensitive files. It is extremely important to take all the necessary measures to keep all the information and the machines themselves secure, as only in this way it will be reasonable to use them.

References

Araujo, R. & Hau, W. (2008). Going Virtual Requires the Right Technology. Retrieved from http://www. softwaremag. com/focus-areas/security/featured-articles/going-virtual-requires-the-right-technology/

Double-Take. (2006). Virtual System Protection. Retrieved from http://www. sunbeltsoftware. com/documents/virtual-system-protection. pdf

Garfinkel, T. & Rosenblum, M. (2005). When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments. Retrieved from http://www. stanford. edu/~talg/papers/HOTOS05/virtual-harder-hotos05. pdf

Griffin. (2006, August 16). Virtual Machines: Virtualization vs. Emulation [blog]. Retrieved from http://www. griffincaprio. com/blog/2006/08/virtual-machines-virtualization-vs-emulation. html

Kusnetzky, D. (2009, January 15). When is virtual machine technology the wrong choice? [blog]. Retrieved from http://www. zdnet. com/blog/virtualization/when-is-virtual-machine-technology-the-wrong-choice/638

Virtualization Support. (2008). Retrieved from http://www. ca. com/files/technicaldocuments/virtualization-support-tech-guide. pdf

Whitehouse L. (2011, August 5). VMware Backup Vendor Landscape [blog]. Retrieved from http://www. dataprotectionperspectives. com/2011/08/vmware_backup_vendor_landscape/